Saferinternet.at

Fachstelle digitaler Kinderschutz

LEITFADEN

Digitale Aspekte in Kinderschutzkonzepten

Gefördert durch:

Bundeskanzleramt

Version: Juni 2024

Herausgeber und für den Inhalt verantwortlich:
Österreichisches Institut für angewandte Telekommunikation (ÖIAT)

Safer-Internet-Fachstelle digitaler Kinderschutz

Ungargasse 64-66/3/404, 1030 Wien

digitalerkinderschutz@saferinternet.at

Wien, Juni 2024

Saferinternet.at Fachstelle digitaler Kinderschutz

oiat

Bundeskanzleramt

Inhalt

1. Einleitung

An wen richtet sich dieser Leitfaden und wie kann ich ihn nutzen?

Dieser Leitfaden richtet sich an alle, die sich mit der Erarbeitung von Kinderschutzkonzepten beschäftigen. Er dient als Orientierungshilfe und soll sicherstellen, dass möglichst wenige der für die Lebenswelt von Kindern und Jugendlichen so wichtigen digitalen Aspekte übersehen werden.

Im Rahmen der Erstellung des Leitfadens wurden sechs zentrale Themenbereiche identifiziert: Content-Entwicklung und Medienarbeit, Social-Media-Aktivitäten, Online-Kommunikation mit Kindern und Jugendlichen, Mediennutzung und Medienpädagogik, Medienkompetenz sowie Datenschutz. Für jedes dieser Themenfelder werden damit verbundene potenzielle Risiken beschrieben, Reflexionsfragen zur Selbsteinschätzung zur Verfügung gestellt und mögliche Maßnahmen zur Minimierung dieser Risiken aufgezeigt.

Nicht jeder Aspekt wird für jede Organisation gleichermaßen relevant sein. Darüber hinaus wird das Dokument laufend ergänzt und aktualisiert, um stets den neuen Entwicklungen und Herausforderungen im digitalen Raum gerecht zu werden. Das Dokument erhebt daher keinen Anspruch auf Vollständigkeit. Es soll in erster Linie als Anregung dienen, die wesentlichen digitalen Risiken zu identifizieren und entsprechende Maßnahmen zu ergreifen.

Weshalb sollten Sie sich mit digitalen Themen beschäftigen, wenn Sie ein Kinderschutzkonzept erarbeiten?

Die digitale Welt ist zu einem integralen Bestandteil der Lebensrealität von Kindern und Jugendlichen geworden. Eine direkte Trennung zwischen der Nutzung des Internets, dem „Online-Sein“, und dem analogen „Offline-Sein“ ist kaum noch möglich. Kinder, die mit der Digitalisierung aufwachsen, erleben den Umgang mit digitalen Medien als Normalität. Trotz dieser scheinbaren Selbstverständlichkeit der Nutzung kann jedoch nicht davon ausgegangen werden, dass das Wissen über Mediengefahren und der Schutz der eigenen Privatsphäre automatisch verinnerlicht werden. Die verantwortungsbewusste Nutzung digitaler Medien muss auch von Kindern und Jugendlichen erlernt und erprobt werden. Für eine ganzheitliche Orientierung in Bezug auf digitale Medien gilt es, die individuellen Lebenssituationen, die potenziellen Gefahren, aber auch die Teilhabebedürfnisse der Kinder und Jugendlichen zu berücksichtigen.

Ein kompetenter, bewusster und achtsamer Umgang mit Medien und das Wissen über gesellschaftliche Veränderungen im Kontext der Digitalisierung sind bedeutsam für die Professionalität von Fachkräften in der Interaktion mit Kindern, Jugendlichen und Familien.

In welchen Bausteinen eines Schutzkonzepts müssen wir digitale Aspekte mitdenken?

Alle Maßnahmen innerhalb eines Kinderschutzkonzepts gelten für die digitale Welt gleichermaßen. Online können jedoch noch andere Risiken und Gefahren entstehen, die einen spezifischen Schutz von Kindern und Jugendlichen erfordern. Diesem Aspekt kommt der folgende Leitfaden nach.

Sie sollen dazu anregen, digitale Aspekte in sämtliche Überlegungen und Maßnahmen zum Kinderschutz zu integrieren – sei es bei der Erstellung von Gruppenregeln, der Ausarbeitung von Richtlinien für die Öffentlichkeitsarbeit oder der Entwicklung von Konzepten für die pädagogische Praxis. Ziel ist es, ein sicheres, positives und anregendes digitales Umfeld zu schaffen, in dem Kinder und Jugendliche geschützt sind und gleichzeitig ihre digitalen Kompetenzen ausbauen können.

Ein wesentlicher Ansatzpunkt hierfür ist die aktive Einbindung von Kindern und Jugendlichen selbst. Sie sind die Expert:innen der digitalen Welt, navigieren täglich durch soziale Netzwerke, Online-Spiele sowie digitale Lernangebote und kennen die Trends, Chancen und Risiken oft aus erster Hand. Ihre Erfahrungen, Perspektiven und Ideen sind daher unverzichtbar, um realitätsnahe und wirksame Schutzkonzepte zu entwickeln. Durch ihre Beteiligung fördern wir nicht nur ihre Medienkompetenz und ihr Bewusstsein für digitale Sicherheit, sondern stärken auch ihr Selbstvertrauen und ihre Selbstbestimmung.

Wir schätzen Ihr Feedback!

Helfen Sie uns, den Leitfaden "Digitale Aspekte in Kinderschutzkonzepten" weiterzuentwickeln. Ihre Anregungen und Kommentare sind jederzeit willkommen.

Bitte richten Sie Ihr Feedback an:
digitalerkinderschutz@saferinternet.at

Vielen Dank für Ihre Unterstützung!

2. Content-Entwicklung und Medienarbeit

Content-Entwicklung und Medienarbeit sind essenzielle Bestandteile der Öffentlichkeitsarbeit in der Kinder- und Jugendarbeit. Dabei ist es entscheidend, Strategien zu entwickeln, die nicht nur das positive Image und die Ziele der Organisation fördern, sondern auch sicherstellen, dass der Schutz der Privatsphäre und das Wohl der Kinder und Jugendlichen stets im Mittelpunkt stehen.

2.1 Darstellung von Kindern und Jugendlichen

Die Darstellung von Kindern und Jugendlichen in der Öffentlichkeitsarbeit erfordert besondere Sensibilität. Die folgenden Reflexionsfragen sollen Sie dabei unterstützen, die ethischen und rechtlichen Aspekte zu berücksichtigen. Denn die Interessen und das Wohlbefinden der dargestellten Kinder und Jugendlichen sollte bei allen Abbildungen mitgedacht werden.

Mögliche Risiken

- Falscher Kontext in der Darstellung von Kindern und Jugendlichen, z. B. Jugendliche werden im Zuge einer Drogenberatung fotografiert und diese Fotos werden veröffentlicht. Sie werden dargestellt, als hätten sie ein Drogenproblem.
- Durch eine bestimmte Auswahl von Bildern werden stereotypische Rollenzuschreibungen verstärkt.
- Ein Kind ist in einer Pflegefamilie untergebracht und möchte nicht, dass sein Schulumfeld davon erfährt. Wird der Name dieses Kindes in einer Pressemitteilung oder auf der Website der Organisation genannt, könnte dies zu ungewollter Offenlegung seiner persönlichen Situation führen.

Reflexionsfragen	Mögliche Maßnahmen
■ Wird beim Porträtieren von Kindern und Jugendlichen deren Altersstufe angemessen berücksichtigt? ■ Werden Kinder und Jugendliche in einer Weise dargestellt, die ihre vielfältigen Facetten und Potenziale betont? ■ Wird bei der Darstellung darauf geachtet, Stereotype zu vermeiden? ■ Sind die Kinder und Jugendlichen angemessen bekleidet? ■ Wird bei der Darstellung darauf geachtet, dass keine falschen Botschaften transportiert werden oder falsche Eindrücke entstehen können?	■ Richtlinien für die Darstellung von Kindern und Jugendlichen entwickeln. ■ Kinder und Jugendliche in Entscheidungs- und Handlungsprozesse miteinbeziehen. ■ Anliegen von Kindern und Jugendlichen ernst nehmen und berücksichtigen. ■ Bei der Auswahl von Bildern die Kinder und Jugendlichen der Einrichtung miteinbeziehen (Partizipation). ■ Festlegen von Richtlinien, um die Identität der Kinder zu schützen – Pseudonyme verwenden. (Ausnahme: Die Verwendung des echten Namens erfolgt mit Zustimmung und liegt im Interesse der Kinder/Jugendlichen.)

■ Wird die Privatsphäre aller beteiligten Personen respektiert? ■ Werden Pseudonyme verwendet, um die Identität der Kinder zu schützen?	

2.2 Information und Zustimmung

Wenn Inhalte veröffentlicht werden, die einen Personenbezug zu Kindern und Jugendlichen haben, also z. B. Kinder und Jugendliche auf Bildern erkennbar sind oder in Texten namentlich genannt werden, muss eine schriftliche Einwilligung eingeholt werden. Bis zum 14. Geburtstag wird die Einwilligung sowohl von den betroffenen Kindern und Jugendlichen als auch von deren Erziehungsberechtigen eingeholt. Ab dem 14. Geburtstag reicht die Einwilligung der Kinder und Jugendlichen.

Mögliche Risiken

- Das Veröffentlichen von Bildern oder Daten ohne Einwilligung kann gegen Datenschutzgesetze wie die DSGVO verstoßen, was zu rechtlichen Schritten, Geldstrafen oder anderen Sanktionen führen kann.
- Kinder und Jugendliche könnten sich unwohl oder bloßgestellt fühlen, wenn ihre Bilder oder Informationen ohne ihre Zustimmung verwendet werden.
- Kinder und Jugendliche könnten das Gefühl haben, dass ihre Rechte und ihre Privatsphäre missachtet wurden, was das Vertrauen in die Einrichtung beeinflussen könnte.
- Die Formulierung von Zustimmungserklärungen kann so komplex sein, dass die betroffenen Personen sie nicht vollständig nachvollziehen können. In solchen Fällen wird die Zustimmung zur bloßen Formalität, die ihren eigentlichen Zweck verfehlt.

Reflexionsfragen	Mögliche Maßnahmen
■ Sind die betroffenen Kinder/Jugendlichen und ggf. ihre Erziehungsberechtigen über den Zweck und Umfang der Nutzung ihres Bildes informiert? ■ Wurde eine angemessene bzw. offiziell gültige Zustimmung eingeholt? ■ Wurde die Zustimmung so eingeholt, dass die betroffenen Kinder/Jugendlichen und ggf. ihre Erziehungsberechtigen auch verstehen, was genau sie erlauben?	■ Einwilligungsformulare entwickeln, die speziell auf die Bedürfnisse und das Verständnisniveau von Kindern/Jugendlichen zugeschnitten sind. Diese Formulare sollten alle relevanten Informationen enthalten, einschließlich der Art der Inhalte, den Verwendungszweck, den Veröffentlichungsort etc.

2.4 Partizipation

In der Content-Entwicklung und Medienarbeit ist es oft sinnvoll, Kinder und Jugendliche auch aktiv in den Produktionsprozess miteinzubeziehen. Dabei ist es entscheidend, von Anfang an klare und transparente Spielregeln festzulegen, um Kinder und Jugendliche adäquat zu schützen.

Mögliche Risiken

- Inhalte, die ohne die Beteiligung der Zielgruppe erstellt werden, können deren Bedürfnisse und Interessen verfehlen. Wenn Kinder und Jugendliche das Gefühl haben, dass ihre Stimme und ihre Meinung nicht zählen, kann dies zu Frustration und einem Gefühl der Machtlosigkeit führen.
- Beliebte Medienprodukte in der Jugendarbeit sind sogenannte Takeovers: Dabei übernehmen Jugendliche für kurze Zeit die Social-Media-Accounts der Organisationen/Einrichtungen und posten in deren Namen. Das Ziel solcher Takeovers ist es, auf die tatsächlichen Bedürfnisse der Jugendlichen einzugehen, indem sie die Inhalte selbst gestalten. Während eines Takeovers sind die Kinder/Jugendlichen stärker öffentlich sichtbar, was sie anfälliger für Online-Belästigung, Cybermobbing etc. macht. Die Kinder/Jugendlichen könnten zudem unangemessene Inhalte veröffentlichen und sich selbst oder andere dadurch gefährden oder schädigen.

Reflexionsfragen	Mögliche Maßnahmen
■ Können die Kinder und Jugendlichen ihre Perspektiven in die Content-Entwicklung und Medienarbeit einbringen? ■ Bieten Sie als Einrichtung Schulungs- und Unterstützungsmaßnahmen an, um die Medienkompetenz der Kinder und Jugendlichen zu fördern? ■ Wird regelmäßig Feedback von den Kindern und Jugendlichen eingeholt und für weitere Inhalte berücksichtigt? ■ Welche Maßnahmen werden ergriffen, um die Sicherheit und Privatsphäre der Kinder und Jugendlichen zu schützen, v. a. in Bezug auf das Takeovers?	■ Formulierung und Durchsetzung von klaren Richtlinien, die die Sicherheit und Privatsphäre der Kinder und Jugendlichen gewährleisten – auch von den Kindern und Jugendlichen selbst anzuwenden. ■ Implementierung von Feedback-Systemen, die es Kindern und Jugendlichen ermöglichen, Feedback zu den Inhalten zu geben und eigene Ideen einzubringen (Umfragen, Fokusgruppen, partizipative Workshops etc.). ■ Inhalte, die von Kindern und Jugendlichen erstellt werden, vor der Veröffentlichung überprüfen. ■ Workshops und Schulungen für eine verantwortungsvolle Nutzung und Umsetzung von Medieninhalten (Personal sowie Kinder und Jugendliche).

Weiterführende Materialien

- Saferinternet.at: Selbstdarstellung von Mädchen und Jungs im Internet

- Saferinternet.at: Worauf müssen wir bei einem „Takeover“ auf Instagram & Co. achten?
- Saferinternet.at: Dürfen Fotos/Videos von Schüler:innen auf die Schulwebsite gestellt werden?
- Saferinternet.at: Fotos im Internet – nicht alles ist erlaubt!
- Bundeskanzleramt: Leitfaden zur Erarbeitung von Kinderschutzkonzepten
- Bundes Jugend Vertretung: Kinderrechte in der Berichterstattung
- Kinderbüro – Die Lobby für Menschen bis 14.: Medienleitfaden für eine kindgerechte Berichterstattung

3. Social-Media-Aktivitäten

Social Media dient vielen Organisationen als wichtiger Kommunikationskanal, um vor allem junge Menschen direkt in ihrer digitalen Lebenswelt zu erreichen und mit ihnen in Austausch treten zu können. Zum Schutz von Kindern und Jugendlichen ist es wichtig, grundlegende Verhaltensregeln für die Nutzung von Social Media einzuhalten.

3.1 Social-Media-Kanäle/Zuständigkeiten

Für den erfolgreichen und sicheren Einsatz von Social-Media-Kanälen in der Arbeit mit Kindern und Jugendlichen ist eine klare Definition der Verantwortlichkeiten innerhalb der Organisation entscheidend. Bei der Auswahl der geeigneten Social-Media-Kanäle sollten Organisationen sorgfältig überlegen, welche Plattformen am besten dazu geeignet sind, ihre Zielgruppen effektiv zu erreichen und gleichzeitig ein hohes Maß an Sicherheit und Schutz für Kinder und Jugendliche gewährleistet werden kann.

Mögliche Risiken

- Ein Posting der Organisation, das harmlos und konfliktfrei erscheint, löst am Wochenende plötzlich einen Shitstorm aus (z. B. abgebildetes Kind könnte Hassrede ausgesetzt sein). Das Kind folgt der Organisation und sieht die vielen negativen Kommentare. Die Organisation hat aber am Wochenende geschlossen – keiner kann eingreifen, da die Zugangsdaten fehlen.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche Social-Media-Kanäle werden von der Organisation genutzt und zu welchem Zweck? ■ Welcher Content wird auf den jeweiligen Kanälen veröffentlicht? (siehe „Content-Entwicklung und Medienarbeit“) ■ Welche Zielgruppen werden über die Kanäle angesprochen? ■ Wie sind die Zuständigkeiten innerhalb der Organisation verteilt und wer hat Zugriff auf die einzelnen Kanäle? ■ Wo werden die Zugriffsdaten abgespeichert/hinterlegt? ■ Welche Qualifikationen müssen die zuständigen Personen mitbringen?	■ Gemeinsam (auch mit Kindern und Jugendlichen als Expert:innen) Social-Media-Guidelines und Internet-Policies für die Organisation entwickeln inkl. Dokumentation, welche Kanäle genutzt werden und zu welchem Zweck (z. B. Aufklärungsarbeit, Community-Building, etc.). ■ Festlegen, wer für die Verwaltung und Pflege der Social-Media-Kanäle zuständig ist. (Empfehlung: Mehrere Personen festlegen, die auf die einzelnen Kanäle Zugriff haben; Zuständigkeiten und Vorgehensweise für betriebsfreie Zeiten überlegen) ■ Rollen und Berechtigungen für die zugriffsberechtigen Personen erstellen, um sicherzustellen, dass nur autorisiertes Personal in der Lage ist, Inhalte zu posten oder auf Interaktionen zu reagieren.

	■ Zugriffsdaten sicher abspeichern, z. B. in einem verschlüsselten Passwortmanager. ■ Zuständige Fachkräfte laufend fortbilden, um sicherzustellen, dass sie über aktuelle Trends und Best Practices in den Bereichen „Social Media“ und „digitaler Kinderschutz“ informiert sind.

3.2 „Netiquette“

Der Begriff „Netiquette“ setzt sich aus den Wörtern „Netzwerk“ und „Etikette“ zusammen und bezieht sich auf die Verhaltensregeln und Höflichkeitsnormen, die in der digitalen Kommunikation als angemessen und respektvoll gelten. Diese ungeschriebenen oder manchmal explizit formulierten Regeln helfen dabei, die Interaktionen auf Online-Plattformen respektvoll zu gestalten. Es liegt in der Verantwortung der Organisation, Netiquette-Richtlinien festzulegen und durchzusetzen, um eine sichere und respektvolle Online-Umgebung für Kinder und Jugendliche zu schaffen.

Mögliche Risiken

- Wenn Netiquette-Regeln nicht beachtet oder durchgesetzt werden, können Kommunikationsplattformen schnell zu einem Nährboden für Cybermobbing werden. Kinder und Jugendliche können leichter Opfer von Belästigungen, Beleidigungen und anderen Formen von Online-Missbrauch werden, was langfristige psychische Auswirkungen haben könnte.
- Ein Mangel an Netiquette kann ein allgemein feindseliges und unangenehmes Online-Umfeld schaffen, in dem Kinder und Jugendliche sich unsicher oder unwohl fühlen. Dies kann ihre Bereitschaft, an Online-Aktivitäten teilzunehmen, negativ beeinflussen und zu sozialer Isolation führen.

Reflexionsfragen	Mögliche Maßnahmen
■ Gibt es bereits Netiquette-Richtlinien? ■ Inwieweit werden Kinder und Jugendliche in die Entwicklung und Überarbeitung der Netiquette-Richtlinien einbezogen? ■ Wie wird die Einhaltung der Netiquette auf den einzelnen Kanälen überwacht? Wird Community-Management betrieben? ■ Welche Maßnahmen werden im Krisenfall getroffen (z. B. im Falle von Cybermobbing oder Hassrede)?	■ Netiquette-Richtlinien im partizipativen Prozess mit Kindern und Jugendlichen entwickeln: Verwendung einer angemessenen Sprache; Privatsphäre und Grenzen der Kinder und Jugendlichen respektieren; verantwortungsvolle Gesprächsführung; Berücksichtigung der unterschiedlichen Wirkung von Bildern und Texten auf das Gegenüber. Persönliche Grenzen und das Empfinden ihrer Verletzung können auch im digitalen Raum je nach Person sehr unterschiedlich sein.

■ Wie wird mit fremden Inhalten auf den internen Kanälen umgegangen, wenn diese gegen die Netiquette verstoßen?	■ Moderationsrichtlinien entwickeln, die definieren, wie mit Inhalten umgegangen wird, die gegen die Netiquette verstoßen: Regelmäßige Aufklärung der Community über die geltenden Verhaltensregeln und die Bedeutung des respektvollen Umgangs; Blockierung, Entfernung und Meldung von unangemessenen Inhalten etc. ■ Krisenplan mit klaren Handlungsanleitungen im Falle eines Shitstorms entwickeln. ■ Feedback-Systeme implementieren, die es Nutzer:innen ermöglichen, Feedback zu geben oder Bedenken zu äußern, was die Inhalte und die Kommunikation auf dem Kanal betrifft (z. B. Veröffentlichung einer E-Mail-Adresse, an die sie sich wenden können).

3.3 Freundschaftsanfragen und Follows

Die Regelung von Freundschaftsanfragen und Follows zwischen Fachkräften und Kindern innerhalb eines Kinderschutzkonzepts ist unerlässlich, um professionelle Grenzen zu wahren, die Privatsphäre und Sicherheit der Kinder zu schützen und das Vertrauen in die Integrität der Organisation zu erhalten.

Mögliche Risiken

- Die Interaktion in sozialen Netzwerken kann die professionellen Grenzen zwischen Fachkräften und den ihnen anvertrauten Kindern verwischen. Persönliche Beziehungen auf Plattformen wie Facebook, Instagram oder Snapchat können dazu führen, dass Kinder und Jugendliche oder die erwachsenen Bezugspersonen diese Beziehungen missverstehen oder dass sich unangemessene Beziehungen entwickeln.
- Die direkte private Kommunikation über soziale Medien eröffnet Möglichkeiten für potenziellen Missbrauch oder unangemessenes Verhalten. Kinder könnten aufgrund der asymmetrischen Machtverhältnisse Schwierigkeiten haben, sich gegenüber Fachkräften abzugrenzen.
- Sollte es zu einem Vorfall kommen, in dem eine Fachkraft beschuldigt wird, die Beziehung zu einem Kind über soziale Medien unangemessen gestaltet zu haben, kann dies das Vertrauen in die Organisation ernsthaft schädigen und deren Reputation langfristig beeinträchtigen.

Reflexionsfragen	Mögliche Maßnahmen

■ Gibt es bereits klare Richtlinien, die den Umgang mit Freundschaftsanfragen und Follows definieren? ■ Wo und in welchen Situationen kommt es vor, dass Fachkräfte mit Kindern und Jugendlichen über persönliche Accounts in Kontakt stehen (Freundschaftsanfragen)? ■ Zu welchem Zweck dient dieser persönliche Kontakt? ■ Welche Schritte werden unternommen, um zu überlegen und zu rechtfertigen, warum in diesem Fall eine Freundschaftsanfrage angenommen wird (z. B. im Rahmen von Social Media Guidelines)? ■ Auf welche persönlichen Informationen haben die Fachkräfte und auch die Kinder und Jugendlichen dadurch Zugriff? ■ Wie kann gewährleistet werden, dass die Kommunikation ausschließlich im beruflichen Kontext bleibt? ■ Wie kann sichergestellt werden, dass es den Fachkräften gelingt, die professionelle Distanz auch in emotionalen Situationen zu wahren?	■ Entwicklung und Implementierung von Richtlinien für den Umgang mit Freundschaftsanfragen und Follows (sowohl Organisations-Accounts als auch Privat-Accounts). ■ Wenn möglich, ausschließlich über die Kanäle der Organisation mit den Kindern und Jugendlichen kommunizieren (kann von mehreren Personen eingesehen werden – Mehraugenprinzip). ■ Wenn erforderlich, Ausnahmen und Zweck definieren und klare Richtlinien für diese Fälle festlegen (z. B. Kommunikation ausschließlich im beruflichen Kontext bzw. über Kanäle, die von mehreren Personen eingesehen werden können; regelmäßige Dokumentation über den Austausch etc.). ■ Überprüfung: Jede Freundschaftsanfrage, die angenommen wird, wird vorab geprüft und gerechtfertigt, z. B. gemeinsam im Team oder durch die Kinderschutzbeauftragten der Organisation. ■ Überprüfung der Privatsphäre-Einstellungen, um keine privaten/sensiblen Daten zugänglich zu machen und die professionelle Distanz zu wahren. ■ Möglicher Ansatz zum Umgang mit Freundschaftsanfragen und Follows: Zusätzlich zum privaten Account auch einen beruflichen Account anzulegen, in dem die Fachkraft ausschließlich ihre berufliche Rolle einnimmt. ■ Kommentare und „Gefällt mir“-Angaben zu öffentlichen Inhalten von Kindern sollten auch nur im beruflichen Kontext erfolgen. ■ Regelmäßige Teamreflexion durchführen, z. B. wie die professionelle Distanz gewahrt werden kann.

Weiterführende Materialien

- Saferinternet.at: Welche Sozialen Netzwerke sollen Jugendeinrichtungen nutzen?
- Saferinternet.at: Welche Regeln brauchen wir als Jugendeinrichtung für die Nutzung von Sozialen Netzwerken?
- Saferinternet.at: Mit Shitstorms souverän umgehen
- Steirischer Landesjugendverband: Digitale Jugendarbeit und Social Media

4. Online-Kommunikation mit Kindern und Jugendlichen

Online-Kommunikation kann auf vielen verschiedenen Wegen erfolgen, je nachdem, welche Kommunikationskanäle eine Organisation nutzt, um mit Kindern und Jugendlichen in Kontakt zu treten. Im folgenden Kapitel werden die verschiedenen Aspekte und Herausforderungen digitaler Interaktionen betrachtet, um sicherzustellen, dass diese Kommunikationsformen den Schutz und die Förderung junger Menschen optimal unterstützen.

4.1 Sprache in der Online-Kommunikation

Bei der Online-Kommunikation mit Kindern und Jugendlichen ist es entscheidend, sich stetig mit den neuesten Trends der digitalen Kommunikationskultur auseinanderzusetzen. Dies ermöglicht es, die Sprache der jungen Menschen nicht nur zu verstehen, sondern auch angemessen darauf zu reagieren. Die Online-Sprache der Jugendlichen kann komplex und schwer zu interpretieren sein, weshalb es oft hilfreich ist, Jugendliche selbst als „Übersetzer" miteinzubeziehen, um Missverständnisse zu vermeiden und eine effektive Kommunikation zu gewährleisten.

Mögliche Risiken

- Wenn Fachkräfte die Jugendsprache nicht verstehen, können sie wichtige Inhalte oder Nuancen in der Kommunikation übersehen. Das kann dazu führen, dass sie die Bedürfnisse und Probleme der Kinder und Jugendlichen nicht vollständig erfassen oder falsch interpretieren.
- Kinder und Jugendliche könnten das Gefühl bekommen, dass Fachkräfte sie und ihre Lebenswelt nicht verstehen, was zu einem Mangel an Vertrauen und Offenheit in der Kommunikation führen kann.
- Wenn Fachkräfte zu sehr versuchen, „cool" zu wirken, kann die eigentliche Botschaft ihrer Kommunikation an Gewicht verlieren.

Reflexionsfragen	Mögliche Maßnahmen
■ Verstehen die Fachkräfte den Sprachgebrauch der Kinder und Jugendlichen? Können sie versteckte Hassbotschaften, Abwertungen etc.	■ Bei der Verwendung des Sprachgebrauchs von Kindern und Jugendlichen sollte darauf geachtet werden, keine unangemessenen Sprachelemente zu übernehmen (Gewalt,

erkennen, um entsprechend darauf zu reagieren? ■ Inwiefern bzw. inwieweit wird die eigene Sprache angepasst, um die Kommunikation mit Kindern und Jugendlichen zu erleichtern? ■ Wie halte ich mich über aktuelle Trends und Entwicklungen auf dem Laufenden? ■ Wird auf die unterschiedliche Wirkung von Bildern und Texten geachtet, z. B. bei der Verwendung von Emojis?	sexuelle Inhalte, unangebrachte Insider-Witze etc.). ■ Die Verwendung der „Jugendsprache“ sollte immer überdacht und reflektiert werden, um die professionellen Grenzen wahren zu können. ■ Entwicklung und Implementierung von grundlegenden Haltungsgrundsätzen – auch in Bezug auf die Sprache bzw. Kommunikation. ■ Um das Sprachverständnis und die Fähigkeit zur Erkennung von subtilen Signalen bei Fachkräften in der Jugendarbeit zu verbessern, sollten regelmäßige Schulungen und Workshops angeboten werden. ■ Die aktive Teilnahme an Online-Communitys und Plattformen, die von Jugendlichen frequentiert werden, kann Fachkräften helfen, ein besseres Verständnis für die verwendete Sprache und die kulturellen Kontexte zu entwickeln. Dies sollte jedoch ethisch und unter Wahrung der Privatsphäre und Grenzen der Jugendlichen geschehen. ■ Durch die Durchführung von Rollenspielen können Fachkräfte üben, wie man effektiv auf verschiedene Arten von Kommunikation reagiert. Diese Übungen können helfen, das Bewusstsein für subtile Signale zu schärfen und angemessene Reaktionsstrategien zu entwickeln. ■ Um das Verständnis der Sprache von Kindern und Jugendlichen zu verbessern, ist der direkte Austausch mit der Zielgruppe selbst sehr hilfreich. Hierfür eignen sich Formate, in denen Jugendliche als Expert:innen einbezogen werden, besonders gut, da sie den Fachkräften ermöglichen, aus erster Hand von den Jugendlichen als Expert:innen ihrer eigenen Kultur und Sprache zu lernen.

4.2 Online-Beratung

Die Online-Beratung ist für viele Organisationen ein wichtiger Kommunikationskanal, da sie eine leicht zugängliche und vertrauliche Kommunikationsform bietet, um auf die Bedürfnisse und Anliegen von Kindern und Jugendlichen effektiv eingehen zu können. Im Kontext eines Kinderschutzkonzepts muss der Bereich der Online-Beratung unter dem Aspekt des digitalen Kinderschutzes betrachtet werden, da er spezifische Risiken birgt, die adressiert und minimiert werden müssen, um die Sicherheit und das Wohlergehen von Kindern und Jugendlichen zu gewährleisten.

Mögliche Risiken

- Ohne klare und transparente Kommunikation könnten Kinder, Jugendliche und ihre Betreuer:innen zögern, die Dienste zu nutzen, da sie unsicher sind, was sie erwartet. Dies kann dazu führen, dass Betroffene keine Unterstützung suchen oder erhalten, die sie möglicherweise dringend benötigen.
- Ohne klare Datenschutzrichtlinien und Sicherheitsprotokolle besteht ein erhöhtes Risiko, dass persönliche Informationen ungeschützt bleiben und potenziell missbraucht oder unautorisiert weitergegeben werden. Dies kann rechtliche Konsequenzen für die Organisation haben und das Wohlbefinden der Ratsuchenden beeinträchtigen.

Reflexionsfragen	Mögliche Maßnahmen
■ Wie wird die Vertraulichkeit und Sicherheit der Kommunikation gewährleistet? (siehe Punkt „Datenschutz") ■ Werden Maßnahmen getroffen, um die Authentizität der Berater:innen sicherzustellen? (Authentifizierungsverfahren) ■ Ist für die Kinder und Jugendlichen ersichtlich, mit wem sie kommunizieren? ■ Wie ist die Kontaktaufnahme geregelt? ■ Wie wird gewährleistet, dass die digitalen Beratungsangebote barrierefrei und für alle jungen Menschen zugänglich sind? ■ Welche Personen bzw. wie viele Personen haben Zugriff auf diese Kanäle? ■ Wie wird eine Online-Beratung dokumentiert bzw. aufgezeichnet? ■ Gibt es Kommunikationsrichtlinien für den Bereich der Online-Beratung? ■ Wie wird in Fällen akuter Gefährdung gehandelt, z. B. wenn das Kind bzw. der:die Jugendliche von akuter Gewalt in der Familie spricht? ■ Gibt es Protokolle oder Notfallpläne für unmittelbar erforderliche Interventionen, z. B. bei angekündigtem Suizid?	■ Implementierung von Ende-zu-Ende-Verschlüsselung. ■ Einführung von Authentifizierungsverfahren für Berater:innen, wie z. B. durch Passwörter, biometrische Daten oder Zwei-Faktor-Authentifizierung. ■ Klare Kennzeichnung oder Kommunikation der Identität der Berater:innen für die Kinder und Jugendlichen, z. B. durch Angabe des Namens. ■ Möglichkeiten der Kontaktaufnahme sowie damit verbundene Prozesse transparent darstellen und kommunizieren (Kontaktmöglichkeiten, Erreichbarkeit, Beratungsprozess, Follow-up und weitere Unterstützung, Datenschutzrichtlinien, Feedbackmöglichkeiten etc.). ■ Schulung aller Beteiligten im Umgang mit vertraulichen Informationen und Datenschutzpraktiken. ■ Bereitstellung von Diensten auch in „Leichter Sprache" und mit mehrsprachigen Optionen. ■ Einführung des Mehraugen-Prinzips, indem mehrere Fachkräfte Zugriff auf Kommunikationskanäle haben; regelmäßige Überprüfungen, wer Zugang zu welchen Daten hat. ■ Klare Richtlinien zur Dokumentation und Aufzeichnung von Beratungsgesprächen,

■ Welche Unterstützungssysteme sind für das Beratungspersonal eingerichtet, um mit der emotionalen Belastung umgehen zu können?	einschließlich Datenschutzbestimmungen; sichere Speicherung von Dokumentationsmaterialien in Übereinstimmung mit gesetzlichen Vorgaben. ■ Erstellung und Durchsetzung spezifischer Kommunikationsrichtlinien für Online-Beratungen. ■ Erarbeitung und Implementierung von Notfallplänen für unmittelbar erforderliche Interventionen. ■ Klare Anweisungen für das Vorgehen in Krisensituationen. ■ Bereitstellung von psychologischer Unterstützung und Supervision für Berater:innen.

4.3 Informelle 1:1-Kommunikation

Informelle 1:1-Kommunikation zwischen Betreuungspersonen und Kindern und Jugendlichen, wie beispielsweise in einer Wohngemeinschaft oder zwischen Fußballtrainer:in und Spieler:in, muss im Rahmen eines Kinderschutzkonzepts sorgfältig betrachtet werden, um sicherzustellen, dass solche Interaktionen die Sicherheit und das Wohlbefinden der Kinder und Jugendlichen unterstützen und kein Raum für Missbrauch oder unangemessenes Verhalten entsteht.

Mögliche Risiken

- Übergriffiges Verhalten einer Autoritätsperson (Trainer:in, Betreuer:in etc.)
- Unter Druck setzen der Kinder und Jugendlichen durch eine Autoritätsperson. Beispiel aus dem Sportbereich: Kinder und Jugendliche überschreiten intuitiv empfundene Grenzen, motiviert durch das Ziel, sich zu verbessern und bisherige Leistungsgrenzen zu überwinden. Diese Dynamik kann es ihnen erschweren, klar und bestimmt „Stopp“ oder „Halt“ zu sagen, insbesondere wenn sie mit unangemessenen Verhaltensweisen oder gar sexuellen Übergriffen durch Trainer:innen oder Betreuer:innen konfrontiert werden.
- Privates und berufliches Verhältnis zwischen Kindern/Jugendlichen und Autoritätsperson verschwimmt.

Reflexionsfragen	Mögliche Maßnahmen
■ Wo findet 1:1-Kommunikation mit Kindern und Jugendlichen in der Organisation statt?	■ Wenn möglich, 1:1-Kommunikation gänzlich vermeiden, indem z. B. Online-Gruppen

Wer führt diese durch und welche Gründe gibt es für die 1:1-Kommunikation? ■ Wie wird die Angemessenheit der 1:1-Kommunikation regelmäßig bewertet? ■ Mit welchen Geräten wird die 1:1-Kommunikation durchgeführt? Mit privaten Geräten oder Diensthandys? ■ Ist die 1:1-Kommunikation für andere Kolleg:innen transparent? Haben mehrere Kolleg:innen Einsicht in die Kommunikationsverläufe? ■ Wird die 1:1-Kommunikation dokumentiert bzw. aufgezeichnet? ■ Wie werden die Rahmenbedingungen für die 1:1-Kommunikation festgelegt und überwacht? ■ Gibt es klare Verfahren für die Meldung und Behandlung von Bedenken oder Missständen in der 1:1-Kommunikation? ■ Wie wird die Vertraulichkeit in der 1:1-Kommunikation gewahrt und welche Ausnahmen gibt es? ■ Unter welchen Umständen dürfen oder müssen Informationen aus der 1:1-Kommunikation mit anderen geteilt werden? ■ Wie wird sichergestellt, dass solche Entscheidungen transparent und im besten Interesse der Kinder oder Jugendlichen sind?	genutzt werden oder andere Erwachsene (Eltern, Kolleg:innen etc.) miteingebunden werden. ■ Entwicklung und Implementierung klarer Richtlinien, die den Umfang und die akzeptablen Formen der 1:1-Kommunikation definieren. Diese Richtlinien sollten spezifisch darauf eingehen, was als angemessene Kommunikation gilt und was nicht. ■ Fortbildungen zur Sensibilisierung bezüglich der Risiken und Herausforderungen der 1:1-Kommunikation und wie man diese effektiv handhabt. ■ Regelmäßige Überprüfungen und Feedback-Sitzungen mit den Mitarbeitenden, um sicherzustellen, dass die Kommunikation den festgelegten Standards entspricht und um mögliche Probleme frühzeitig zu identifizieren. ■ Verwendung von diensteigenen Geräten und Plattformen für alle 1:1-Kommunikationen, um die Sicherheit und Nachverfolgbarkeit zu gewährleisten. ■ Einrichtung eines leicht zugänglichen Beschwerdeverfahrens, das es Kindern und Jugendlichen sowie deren Eltern ermöglicht, Bedenken oder Beschwerden sicher und vertraulich zu melden. ■ Etablierung einer Kultur der Offenheit und Transparenz, in der Kinder und Jugendliche ermutigt werden, über ihre Erfahrungen und etwaige Bedenken zu sprechen. ■ Regelmäßige Diskussionen und Feedback-Runden mit Kindern und Jugendlichen, um ihre Perspektiven zu hören und daraus zu lernen.

4.4 Peer-Beratung

Unter Peer-Beratung versteht man eine Form der Unterstützung, bei der Personen aus derselben Gruppe oder mit ähnlichen Erfahrungen einander beraten und helfen. In vielen Fällen wird sie unter Gleichaltrigen (Peers) durchgeführt, was bedeutet, dass die Beratenden und die Beratenen sich in ähnlichen Lebensphasen oder Situationen befinden.

Bieten Organisationen diese Form der Unterstützung an, muss sie im Rahmen eines Kinderschutzkonzepts ebenfalls sorgfältig überprüft werden, um sicherzustellen, dass sowohl das Wohlbefinden der beratenden Jugendlichen als auch der hilfesuchenden Jugendlichen geschützt wird.

Mögliche Risiken

- Überforderung der Peers durch Schilderungen der Hilfesuchenden.
- Übergriffiges Verhalten von Peers oder Hilfesuchenden, z. B. indem eine Ausnahmesituation zum eigenen Vorteil ausgenutzt wird.

Reflexionsfragen	Mögliche Maßnahmen
■ Wie wird sichergestellt, dass die Peer-Berater:innen für die Beratung anderer Peers qualifiziert sind? ■ Werden den Peers Möglichkeiten zur Supervision geboten? ■ Gibt es eine klare Definition der Rolle des:der Peer-Berater:in? Ist der Aufgabenbereich klar abgegrenzt? ■ Wie werden die Peer-Berater:innen ausgewählt? ■ Findet die Peer-Beratung als 1:1-Kommunikation statt (siehe Punkt „Online-Beratung“) oder in der Gruppe? ■ Gibt es einen Austausch zwischen den Peer-Berater:innen, um über Erfahrungen sprechen zu können? (Intervision)	■ Umfassende Schulung zu Themen wie Gesprächsführung, Datenschutz, Umgang mit Krisensituationen und Kenntnisse über Weitervermittlungsmöglichkeiten. ■ Definition und Kommunikation der spezifischen Rolle und Aufgaben der Peer-Beratung, um sicherzustellen, dass Grenzen eingehalten werden (auch zum Selbstschutz). ■ Regelmäßige Supervision: Bereitstellung regelmäßiger Supervisionssitzungen, in denen Peer-Berater:innen ihre Fälle mit erfahrenen Supervisor:innen besprechen können. ■ Bestimmung des Beratungsformats: Entscheidung, ob die Peer-Beratung in Einzelgesprächen oder in Gruppensettings stattfindet, abhängig von den Zielen und Ressourcen des Programms. ■ Einrichtung von Intervisionsgruppen: Organisation regelmäßiger Treffen, in denen Peer-Berater:innen ihre Erfahrungen austauschen und voneinander lernen können.

	■ Feedback bei den Ratsuchenden einholen.

4.5 Digitale Räume & Online-Veranstaltungen

Auch in der Kinder- und Jugendarbeit ist die Digitalisierung angekommen. Aufgrund der Coronavirus-Pandemie und den damit verbundenen Einschränkungen für persönlichen Treffen ergab sich die Notwendigkeit, auf digitale Angebote und Formate umzustellen. Um einen selbstbestimmten und sicheren Umgang mit digitalen Medien zu entwickeln und die Chancen der Digitalisierung für möglichst viele Kinder und Jugendlichen nutzbar zu machen, ist es erforderlich und sinnvoll, sich mit einem reflektierten Blick dem Bereich der digitalen Jugendarbeit anzunähern.

Mögliche Risiken

- Unangemessene Inhalte: Die Gefahr, dass Kinder und Jugendliche auf schädliche oder ungeeignete Inhalte stoßen, die durch andere Nutzer:innen geteilt/veröffentlicht wurden.
- Cybermobbing: Digitale Räume können für Belästigungen und Mobbing missbraucht werden.
- Mangelnde Aufsicht: Ohne geeignete Aufsicht können digitale Veranstaltungen zu Verhaltensweisen führen, die das Wohl der Teilnehmenden gefährden.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche digitalen Plattformen (z. B. Discord, Teams etc.) werden genutzt bzw. für welchen Zweck werden die Online-Veranstaltungen durchgeführt? ■ Wie transparent und zugänglich sind Informationen über den Zweck und die Ziele der Online-Veranstaltungen für Teilnehmer:innen und deren Erziehungsberechtigte? ■ Welche Datenschutzmaßnahmen sind für digitale Plattformen implementiert, um die persönlichen Informationen der Jugendlichen zu schützen? ■ Wie werden digitale Räume überwacht, um sicherzustellen, dass sie frei von Missbrauch und Belästigung sind? ■ Gibt es bereits Verhaltensrichtlinien für die Nutzung dieser digitalen Plattformen? ■ Inwieweit werden die Kinder und Jugendlichen in die Entwicklung und	■ Auswahl von Plattformen und Tools: Überprüfung der Datenschutzrichtlinien der Plattform, um sicherzustellen, dass sie mit den geltenden Datenschutzgesetzen konform sind und die Privatsphäre der Kinder und Jugendlichen schützen. ■ Implementierung von Ende-zu-Ende-Verschlüsselung auf allen Kommunikationsplattformen, um die Datenübertragung zu sichern. ■ Einsatz von Moderations- und Filtertools, um unangemessene Inhalte oder Verhaltensweisen schnell zu identifizieren und zu entfernen. ■ Entwicklung klarer Verhaltensrichtlinien, die speziell auf die digitale Umgebung zugeschnitten sind und allen Beteiligten bekannt gemacht werden, z. B. welche Inhalte dürfen innerhalb von WhatsApp-Gruppen geteilt werden; welche Inhalte dürfen außerhalb der Gruppe weitergeleitet bzw. geteilt werden etc.

Überarbeitung der Verhaltensrichtlinien einbezogen? ■ Wie wird die Einhaltung dieser Richtlinien auf den einzelnen Kanälen überwacht? Wird Community-Management betrieben? ■ Wer ist für das Community-Management verantwortlich? ■ Welche Maßnahmen werden im Krisenfall getroffen (z. B. im Falle von Cybermobbing oder Hassrede)? ■ Wie wird mit fremden Inhalten auf den internen Kanälen umgegangen, wenn diese gegen die Verhaltensrichtlinien verstoßen? ■ Welche Rechte besitzen die Nutzer:innen bzw. Besucher:innen der digitalen Räume bzw. Online-Veranstaltungen? (Teilen des Bildschirms, Veröffentlichung von Inhalten, Kommentieren etc.) ■ Werden die Nutzungsrechte und Verhaltensrichtlinien klar und verständlich für alle Beteiligten kommuniziert?	■ Einbeziehung von Jugendlichen in die Entwicklung und Überarbeitung von Verhaltensrichtlinien, um sicherzustellen, dass ihre Bedürfnisse und Perspektiven berücksichtigt werden. ■ Einrichtung eines Community-Management-Teams, das für die Einhaltung dieser Richtlinien verantwortlich ist und als Ansprechpartner für die Nutzer:innen dient. ■ Implementierung von Feedback-Mechanismen, die es Jugendlichen ermöglichen, ihre Meinungen und Bedenken anonym oder offen zu äußern. ■ Entwicklung eines Krisenreaktionsplans, der spezifische Schritte und Verfahren für den Umgang mit Vorfällen wie Cybermobbing oder Hassrede umfasst. ■ Einsatz von Moderator:innen in Echtzeit, um digitale Veranstaltungen und Räume zu überwachen. ■ Bei organisationseigenen Apps oder externen Apps, die zur Organisation genutzt werden (z. B. im Kindergarten oder in der Schule): Sicherstellen, dass keine sensiblen Daten auf private Geräte heruntergeladen werden können oder anders exportiert werden können). ■ Sicherstellung der Barrierefreiheit aller digitalen Angebote, um Inklusion zu fördern. ■ Regelmäßige Evaluation der digitalen Angebote durch externe und interne Reviews, um ihre Qualität zu sichern und kontinuierlich zu verbessern. ■ Förderung von Innovationsräumen, in denen Fachkräfte und Kinder/Jugendliche neue Ideen entwickeln und testen können, mit einer Kultur, die Fehler als Lernmöglichkeiten sieht.

	■ Implementierung von Zugriffs- und Benutzerrollen (ev. Möglichkeiten einschränken: Bildschirmteilung, Kommentare, Veröffentlichung von Inhalten etc.). ■ In digitalen Räumen und Veranstaltungen, die speziell für Kinder und Jugendliche konzipiert sind, kann eine klare Identifizierung helfen, die Sicherheit zu gewährleisten, indem sichergestellt wird, dass nur autorisierte und geeignete Personen Zugang erhalten.

Weiterführende Materialien

- Saferinternet.at: Peers in der Jugendarbeit: Großes Finale von make-IT-safe 2.0
- Saferinternet.at: „Gleich und gleich gesellt sich gerne“
- Saferinternet.at: Fragen und Antworten rund um Peer-Programme
- Saferinternet.at: Welche Sozialen Netzwerke sollen Jugendeinrichtungen nutzen?
- Boja: Leitfaden Digitale Jugendarbeit
- Stadt Wien: Teamtool zur Reflexion Digitaler Kinder- und Jugendarbeit
- Stadt Wien: Wiener Leitlinien für digitale Kinder- und Jugendarbeit
- Steirischer Landesjugendverband: Digitale Jugendarbeit und Social Media

5. Mediennutzung bzw. Medienpädagogik

Das Nutzen von und die Kommunikation mit digitalen Medien zählen zu den wichtigsten Freizeitaktivitäten von Kindern und Jugendlichen und beeinflussen zudem auch Lebensbereiche wie Schule, Arbeit und Familie. Eine kompetente, aktive und altersspezifische Begleitung von Kindern und Jugendlichen bei der Nutzung von bzw. in digitalen Lebenswelten (wie z. B. Social Media, digitale Spiele etc.) durch die Fachkräfte der Kinder- und Jugendarbeit ist daher ein wesentliches Aufgabengebiet.

5.1 Interne Geräte

Die sorgfältige Verwaltung und Nutzung interner Geräte ist in verschiedenen Bereichen der Kinder- und Jugendarbeit von entscheidender Bedeutung. In Bildungseinrichtungen und schulischen Programmen sind interne Geräte unerlässlich für den Zugriff auf Lernmaterialien oder die Teilnahme an virtuellem Unterricht. Auch in der Fremdunterbringung oder in Jugendzentren ist die sorgfältige Verwaltung und Nutzung interner Geräte besonders wichtig, um sicherzustellen, dass die Technologienutzung das Wohlbefinden und die Sicherheit der Kinder und Jugendlichen nicht gefährdet. Darüber hinaus ist es aus kinderrechtlicher Sicht wichtig, Kindern und Jugendlichen, die aus unterschiedlichen Gründen kaum Zugang zu digitalen Räumen haben, die digitale Teilhabe am gesellschaftlichen Leben zu ermöglichen.

Mögliche Risiken

- Jugendliche haben auf Geräten in der Einrichtung Zugang zu ungeeigneten Inhalten und können diese ungehindert nutzen.
- Jugendliche erstellen ungeeignete Inhalte in der Einrichtung, etwa auf den dort vorhandenen Geräten (z. B. Gewaltinhalte).
- Geräte werden durch Schadsoftware beeinträchtigt. Dies kann negative Folgen auf Kinder oder Jugendliche haben, z. B. weil an sie Phishing-Nachrichten geschickt werden.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche internen Geräte sind vorhanden? (Computer, Spielekonsole, Diensthandy etc.) ■ Wer hat Zugang zu diesen Geräten bzw. von wem dürfen sie genutzt werden? ■ Wer ist zuständig für die Verwaltung und Wartung dieser Geräte? ■ Wozu werden die Geräte verwendet? ■ Welche Daten werden auf diesen Geräten gespeichert?	■ Dokumentation aller internen Geräte einschließlich Computer, Spielekonsolen, Diensthandys etc. ■ Klare Verantwortlichkeiten für die Verwaltung und Wartung der Geräte bestimmen: Regelmäßige Updates, Überprüfung auf Schadsoftware, allgemeine Instandhaltung etc. ■ Zugriffsbeschränkungen: Definition klarer Richtlinien, wer auf welche Geräte zugreifen darf und zu welchem Zweck.

■ Auf welche Daten haben Personen, die diese Geräte nutzen, Zugang? ■ Welche Schulungen und Richtlinien existieren für das Personal oder die Kinder/Jugendlichen in Bezug auf die Nutzung dieser Geräte? ■ Wie wird innerhalb der Organisation kommuniziert? Werden dazu interne, von der Organisation zur Verfügung gestellte, Geräte verwendet? Welche Informationen werden ausgetauscht? Gibt es dazu eigene Richtlinien?	■ Sicherheitssoftware: Einsatz von Antivirus-Programmen, Firewalls ■ Schulung der Kinder/Jugendlichen und des Personals im sicheren Umgang mit den Geräten. ■ Klare Richtlinien für die Nutzung definieren, die auch den Umgang mit Daten und den Zugriff auf das Internet regeln. ■ Sicherstellen, dass alle sensiblen Daten auf den Geräten verschlüsselt sind und regelmäßig gesichert werden. ■ Einstellungen zum technischen Kinderschutz treffen (z. B. im Betriebssystem oder in den Apps, durch Programme und Apps von Drittanbietern etc.). ■ Regeln bzw. Verhaltensrichtlinien festlegen, etwa welche Informationen mit internen Geräten ausgetauscht werden dürfen (z. B. interne WhatsApp-Gruppe).

5.2 Persönliche Geräte

Die Nutzung persönlicher Geräte durch Fachkräfte sowie Kinder und Jugendliche in der Kinder- und Jugendarbeit wirft wichtige Fragen bezüglich Sicherheit, Datenschutz und verantwortungsvoller Verwendung auf. Dabei ist wichtig, bestehende Richtlinien und Praktiken zu überprüfen, um eine effektive und sichere Handhabung persönlicher Geräte zu gewährleisten.

Mögliche Risiken

- Das Mehraugen-Prinzip kann nicht eingehalten werden, da für die Arbeit die persönlichen Geräte der Fachkräfte genutzt werden.
- Es werden nachteilige Bilder von Kindern und Jugendlichen mit den persönlichen Geräten aufgenommen, die dann im privaten Bereich gezeigt werden.
- Zugang zu unangemessenen Inhalten: Ohne geeignete Kontrollen könnten Kinder und Jugendliche leicht Zugang zu schädlichen oder altersunangemessenen Inhalten erhalten.

Reflexionsfragen	Mögliche Maßnahmen
■ Gibt es klare Richtlinien für die Nutzung persönlicher Geräte im Rahmen der Kinder- und Jugendarbeit?	■ Private Geräte sicher in den Organisationsbetrieb zu integrieren, ist meist aufwendiger, als den Fachkräften

■ Dürfen während der Betreuungssituation Fotos mit den privaten Geräten gemacht werden? Wie wird mit diesen Bildern umgegangen? (siehe Punkt „Datenschutz“) ■ Werden private Handynummern an Kinder und Jugendliche weitergegeben. z. B. in Wohngemeinschaften oder Jugendzentren? ■ Ab wann bekommen Kinder ihr eigenes Handy? (Sozialpädagogische Einrichtungen) Wer trägt die Kosten und die Verantwortung? Wie wird der Umgang mit den Geräten der Kinder und Jugendlichen gehandhabt? Gibt es Regeln? ■ Gibt es Kontrollen durch Fachkräfte und wenn ja, welche und warum? ■ Wie wird innerhalb der Organisation kommuniziert? Werden dazu private Geräte verwendet? Welche Informationen werden ausgetauscht? Gibt es dazu eigene Richtlinien?	Dienstgeräte zur Verfügung zu stellen – wenn möglich, allen Fachkräften Diensthandys zur Verfügung stellen. Dadurch können Einstellungen von der Organisation vorgenommen und überprüft werden. ■ Wenn die Bereitstellung von Dienstgeräten nicht möglich ist: Klare Richtlinien erstellen und regelmäßige Schulungen zu Datenschutzbestimmungen und dem sicheren Umgang mit persönlichen Geräten durchführen. Wenn möglich, zusätzlich technische Sicherheitsmaßnahmen treffen: Passwortschutz, Verschlüsselungen etc. ■ Keine privaten Nummern weitergeben. Wenn die Bereitstellung eines Diensthandys nicht möglich ist, eventuell zweite SIM-Karte zur Verfügung stellen oder Gruppenchats (z. B. in einer Wohngruppe) in Messenger-Diensten erstellen und Telefonnummern verbergen. ■ Regeln bzw. Verhaltensrichtlinien festlegen, z. B. keine Fotos mit privaten Geräten machen; welche Informationen dürfen mit privaten Geräten ausgetauscht werden etc.

5.3 Netzwerkzugang

Kinder und Jugendliche haben ein Recht auf (kindgerechte) Information, auf Beteiligung und freie Meinungsäußerung. Ein Recht auf Internetzugang besteht nicht, dieser wird aber – genau wie Medienkompetenz – immer wichtiger für die gesellschaftliche Teilhabe.

Mögliche Risiken

- Ohne entsprechende Filter oder Überwachungsmaßnahmen können Kinder und Jugendliche leicht auf unangemessene oder schädliche Inhalte wie Pornografie, Gewaltdarstellungen, Hassreden und extremistische Inhalte zugreifen.
- Die unbegrenzte und unregulierte Nutzung von Internet und digitalen Medien kann zu exzessivem Verhalten führen, das süchtig machen und negative Auswirkungen auf die physische und psychische Gesundheit haben kann. Dies äußert sich möglicherweise in schlechtem Schlaf, mangelnder körperlicher Aktivität oder auch in sozialer Isolation.

Reflexionsfragen	Mögliche Maßnahmen

■ Wird in der Einrichtung WLAN zur Verfügung gestellt? ■ Gibt es Regeln für die Nutzung des WLANs, z. B. Nutzungsdauer, „Offline-Zeiten“ etc.? ■ Wer ist zuständig für die Verwaltung? ■ Wer hat Zugriff? ■ Gibt es Sicherheitsmaßnahmen, um unbefugten Zugriff zu verhindern? ■ Gibt es Content-Filter bzw. Sperren? ■ Wie ist das WLAN außerhalb der Öffnungszeiten geregelt? Brauchen die Kinder und Jugendlichen das entsprechende WLAN als Infrastruktur-Versorgung in der Region, weil sie sonst kein anderes zur Verfügung haben?	■ Festlegen von Verantwortlichkeiten: Bestimmen von mehreren Personen, die für die Verwaltung des WLANs zuständig sind. ■ Passwortgeschützter WLAN-Zugang ■ Definieren Sie klare Regeln für die WLAN-Nutzung, einschließlich zulässiger Nutzungszeiten, „Offline-Zeiten“ zur Förderung nicht-digitaler Aktivitäten und Richtlinien zu herunterladbaren Inhalten. ■ Richten Sie Firewalls und Antivirus-Software ein, um das Netzwerk vor externen Angriffen und Malware zu schützen. ■ Setzen Sie Content-Filter ein, um den Zugriff auf unangemessene und schädliche Inhalte zu blockieren.

5.4 Nutzung und Auswahl von Online-Tools, Anwendungen etc.

In der Arbeit mit Kindern und Jugendlichen werden zunehmend digitale Ressourcen eingesetzt, die sowohl in der Freizeit als auch im pädagogischen Kontext eine immer größere Rolle spielen. Für einen verantwortungsvollen Umgang ist die Auswahl geeigneter Online-Tools bzw. Anwendungen entscheidend. Besonderes Augenmerk sollte dabei auf die potenziellen Risiken bestimmter Anwendungen gelegt werden, wie z. B. solche, die für Deep-Fake-Erstellungen genutzt werden können. Darüber hinaus wird der Umgang von Fachkräften mit Alterskennzeichnungen, Altersfreigaben und Altersbeschränkungen sozialer Medien thematisiert. Die angeführten Maßnahmen und weiterführenden Materialien dienen als Orientierung für Fachkräfte, um sicherzustellen, dass die Nutzung digitaler Ressourcen in der Kinder- und Jugendarbeit effektiv, sicher und im besten Interesse der betreuten Kinder und Jugendlichen gestaltet wird.

Mögliche Risiken

- Die Nutzung von Tools wie Deep-Fake-Anwendungen kann zu Cybermobbing und Verunglimpfung führen. Kinder und Jugendliche können sowohl Opfer als auch Täter solcher Handlungen werden, was nicht nur ernsthafte emotionale und psychologische Folgen haben kann, sondern auch strafrechtliche Konsequenzen nach sich zieht, insbesondere wenn diese Handlungen den Ruf einer Person öffentlich schädigen und klar nachweisbar sind.
- Wenn Fachkräfte nicht genügend über Altersbewertungssysteme wie PEGI und USK informiert sind oder unsicher sind, wie sie bei Regelverstößen vorgehen sollen, mangelt es an der notwendigen

Unterstützung und Begleitung, die erforderlich ist, um ein sicheres Umfeld für Kinder und Jugendliche zu schaffen.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche Online-Tools bzw. Anwendungen zur Verfügung gestellt? ■ Wie wird die Auswahl getroffen? ■ Welche Tools werden genutzt, die eventuell Schaden zufügen könnten, z. B. Deep-Fake-Tools, die dann zur Belästigung/Verunglimpfung anderer Jugendlicher genutzt werden? ■ Wie werden die Online-Tools bzw. Anwendungen finanziert? Auf welchen Geräten werden sie genutzt? ■ Wie wird mit Alterskennzeichnungen umgegangen? ■ Wie geht man mit Altersfreigaben um, wenn sich Kinder und Jugendliche von Spielen angesprochen fühlen, für die sie eigentlich noch zu jung sind? t ■ Ist das Personal mit PEGI und USK vertraut? ■ Wie wird mit den Altersbeschränkungen sozialer Medien umgegangen? ■ Melden sich Kinder/Jugendliche an, obwohl sie zu jung sind? ■ Wie wird reagiert, wenn sich Kinder/Jugendliche trotzdem anmelden? ■ Gibt es Regeln bei der Nutzung (Dauer, Inhalte etc.)? ■ Wie wird mit übermäßigem Medienkonsum von Kindern und Jugendlichen umgegangen? ■ Wie werden Eltern über die Medienaktivitäten ihrer Kinder informiert und in diese miteinbezogen?	■ Prozess zur Bewertung und Auswahl von Online-Tools bzw. Anwendungen etablieren. ■ Gemeinsamen Mediennutzungsvertrag mit den Kindern und Jugendlichen als Gesprächsgrundlage ausarbeiten. ■ Informieren: App bzw. soziale Netzwerke kennenlernen; Kinder/Jugendliche fragen, warum sie dies nutzen möchten, welche Altersbestimmungen geben die einzelnen Plattformen vor? (Nicht gleich verbieten, sondern darüber reden.) ■ Gemeinsam anmelden: Nicknamen wählen, der nicht auf das Geschlecht, Alter oder die Identität hinweist. ■ Gemeinsam Privatsphäre-Einstellungen durchgehen. ■ Regeln vereinbaren: Welche Inhalte können veröffentlich werden, welche nicht? ■ Regelmäßig darüber sprechen und nachfragen. ■ Fachkräfte über Systeme wie PEGI und USK aufklären und sicherstellen, dass diese Informationen effektiv an die Kinder und Jugendlichen weitergegeben werden. ■ Sicherstellen, dass Erziehungsberechtigte über die Medienaktivitäten ihrer Kinder informiert werden. ■ Schulungen für Erziehungsberechtigte anbieten, um sie in die digitale Erziehung ihrer Kinder miteinzubeziehen.

Weiterführende Materialien

- Saferinternet.at: Offenes WLAN – worauf müssen wir achten?
- Saferinternet.at: Was bedeuten die Kennzeichen PEGI und USK?
- Saferinternet.at: Müssen wir auf den Computern Filter und Sperren einrichten?

- Saferinternet.at: Wie richte ich einen technischen Kinderschutz ein?
- Saferinternet.at stellt Fachkräften, Erziehungsberechtigten sowie Kindern und Jugendlichen eine Reihe von Informationsmaterialien zu unterschiedlichen Safer-Internet-Themen bereit. Alle Unterrichtsmaterialien, Ratgeber, Folder, Comics etc. finden Sie zum kostenlosen Bestellen oder Downloaden.
- SOS-Kinderdorf: Medienpädagogik in der Kinder- und Jugendhilfe
- SOS-Kinderdorf: Recht Digital – Sicher durch die Aufsichtspflicht im Internet

6. Medienkompetenz

Die Förderung der Medienkompetenz ist ein zentraler Bestandteil des Kinderschutzkonzepts in der Jugendarbeit, da sie sicherstellt, dass sowohl Fachkräfte als auch Kinder und Jugendliche befähigt sind, die Herausforderungen und Risiken der digitalen Welt zu verstehen und verantwortungsvoll damit umzugehen.

6.1 Kompetenzen und Bildung

Medienkompetenz in der Jugendarbeit umfasst mehrere Dimensionen: das Verstehen und die Nutzung verschiedener Medienformen und Technologien, das Bewusstsein über die Risiken und Chancen, die diese Medien bieten, sowie die Fähigkeit, eigene digitale Inhalte kreativ und sinnvoll zu gestalten. Dazu gehört auch das Verständnis der Fachkräfte für Fragen des Datenschutzes, des Urheberrechts und des persönlichen Rechts am eigenen Bild.

Zur Förderung der Medienkompetenz gibt es mittlerweile zahlreiche Fortbildungsmöglichkeiten, die Fachkräften helfen, auf dem neuesten Stand der digitalen Lebenswelten und pädagogischen Methoden zu bleiben. Einige dieser Fortbildungsmöglichkeiten sind in den unten angeführten Materialien ersichtlich.

Mögliche Risiken

- Kinder und Jugendliche, die nicht ausreichend über die Risiken des Internets aufgeklärt sind, können leichter Opfer von Cybermobbing oder Online-Belästigung werden.
- Mangelnde Fähigkeiten, Quellen zu überprüfen und Informationen kritisch zu bewerten, können dazu führen, dass Fachkräfte sowie Kinder und Jugendliche Fehlinformationen verbreiten oder ihnen Glauben schenken.
- Unkenntnis über Urheberrecht und das Recht am eigenen Bild kann dazu führen, dass Fachkräfte, aber auch Kinder und Jugendliche unwissentlich gesetzliche Bestimmungen verletzen, indem sie urheberrechtlich geschütztes Material verwenden oder unerlaubt Bilder von anderen verbreiten.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche Kompetenzen gibt es auf Seiten der Fachkräfte, z. B. aktuelles Wissen über die digitale Lebenswelt der Kinder und Jugendlichen? ■ Welche Kompetenzen gibt es auf Seiten der Kinder/Jugendlichen, z. B. über Cybergrooming, Sexting, Cybermobbing etc.?	■ Fortlaufende Fortbildungen für Fachkräfte: Schulungen und Weiterbildungsmaßnahmen zur digitalen Lebenswelt von Kindern und Jugendlichen, zu aktuellen Entwicklungen usw. ■ Fachkräften Materialien für das Selbststudium zur Verfügung stellen (Literatur, Fachzeitschriften, hilfreiche Links, Online-Webinare etc.).

■ Werden regelmäßige Schulungen in Anspruch genommen bzw. durchgeführt? ■ Wie halten sich die Fachkräfte bezüglich der neuesten Entwicklungen und Trends in der digitalen Welt auf dem Laufenden? ■ Wie erfolgt der Wissenstransfer innerhalb des Teams? ■ Welche Plattformen oder Systeme werden verwendet, um Wissen und Informationen innerhalb des Teams effektiv zu teilen? ■ Welche Unterstützungssysteme stehen für die Fachkräfte zur Verfügung, wenn sie auf komplexe oder herausfordernde Situationen in der digitalen Jugendarbeit stoßen? ■ Welche Ressourcen und Schulungen werden Eltern bzw. Erziehungsberechtigen angeboten, um sie in die Medienbildung ihrer Kinder miteinzubeziehen?	■ Interne Wissensplattformen implementieren, um Wissen und Informationen für alle zugänglich zu machen und auszutauschen. ■ Unterstützungssysteme anbieten: Supervision oder Intervision als professionelle Ressource für die Fachkräfte. ■ Fortlaufende Aufklärungsarbeit bzw. Präventionsarbeit für die Kinder und Jugendlichen anbieten, etwa zu Themen wie Cybergrooming, Sexting, Cybermobbing, Cybercrime, Medienkompetenz etc. ■ Peer-Education-Modelle etablieren, in denen Kinder und Jugendliche voneinander lernen können: Zum Beispiel einen guten Umgang miteinander, eine verantwortungsvolle Mediennutzung und auch wie Mobbing von vornherein verhindert werden kann. ■ Informationsveranstaltungen für Eltern: Regelmäßige Informationsveranstaltungen und Workshops für Eltern und Erziehungsberechtigte anbieten. ■ Ressourcenbereitstellung: Leitfäden, Online-Ressourcen und Zugang zu Beratungsstellen zur Verfügung stellen, um die Eltern bzw. Erziehungsberechtigen in der Medienbildung ihrer Kinder zu unterstützen. ■ Eltern-Kind-Workshops: Gemeinsame Workshops für Eltern und Kinder anbieten, die das gemeinsame Lernen und Diskutieren über sichere Internetnutzung und Medienkompetenz fördern.

6.2 Verantwortung und Unterstützung

In der Arbeit mit Kindern und Jugendlichen ist es entscheidend, dass Fachkräfte als verlässliche Ansprechpartner:innen agieren und aktiv die Mediennutzung begleiten, um eine sichere und positive Online-Erfahrung zu fördern. Dieses Engagement umfasst das Verständnis neuer Medientrends, eine ausgewogene Haltung gegenüber digitalen Medien und die Sensibilisierung der Kinder und Jugendlichen für potenzielle Online-Risiken.

Mögliche Risiken

- Ohne klare Ansprechpartner:innen oder Vertrauenspersonen haben Kinder und Jugendliche möglicherweise niemanden, an den sie sich bei Problemen oder Bedenken wenden können, was zu ungelösten Problemen oder Konfliktsituationen führen kann.
- Wenn sich Fachkräfte ihrer Vorbildfunktion nicht bewusst sind, können sie unbeabsichtigt Verhaltensweisen fördern, die nicht im besten Interesse der Kinder und Jugendlichen sind.
- Eine übermäßig risikofokussierte Sicht auf Medien kann dazu führen, dass Chancen für pädagogisch wertvolle Erfahrungen verpasst werden. Umgekehrt kann eine zu unkritische Haltung dazu führen, dass Risiken übersehen werden.

Reflexionsfragen	Mögliche Maßnahmen
■ Gibt es eine Ansprechperson bzw. eine Vertrauensperson, an die sich die Kinder und Jugendlichen wenden können? ■ Setzen sich die Fachkräfte aktiv mit der Mediennutzung der Kinder und Jugendlichen auseinander? ■ Wie werden neue Medientrends und -technologien evaluiert, um deren Einfluss auf die Zielgruppe zu verstehen und angemessen darauf zu reagieren? ■ Wie sieht die Haltung der Fachkräfte gegenüber digitalen Medien aus? Wie sehen sie Medien – eher als Risiko oder eher als Teil der Lebenswelt von Kindern und Jugendlichen? ■ Wie stehen die Fachkräfte zu dem Ziel, Kinder und Jugendliche zu befähigen, verantwortungsbewusst und kritisch mit Medien umzugehen? ■ Sind sich die Fachkräfte ihrer Vorbildfunktion bewusst? Welche Richtlinien oder Standards setzt die Organisation, um sicherzustellen, dass alle Fachkräfte ihrer Vorbildrolle gerecht werden? ■ Welche Maßnahmen werden ergriffen, um die Kinder und Jugendlichen bezüglich	■ Ansprechperson definieren (ähnlich wie bei Kinderschutzbeauftragten). ■ Mit den Kindern und Jugendlichen im Gespräch bleiben und bei der Mediennutzung begleiten; Offenheit und Interesse zeigen (welche Apps sind gerade im Trend, was macht ihnen Spaß, welche Erfahrungen werden dabei gemacht etc.). ■ Vertrauensvolles und verlässliches Beziehungsverhältnis aufbauen – Kindern und Jugendlichen das Gefühl vermitteln, dass sie eine Ansprechperson in allen Belangen haben. ■ Offene Haltung zu digitalen Lebenswelten signalisieren. ■ Entwicklung und Durchsetzung von Richtlinien, die sicherstellen, dass alle Fachkräfte ihre Vorbildrolle ernst nehmen. ■ Kindern und Jugendlichen Materialien zur Aufklärung und Prävention zur Verfügung stellen (Flyer, Poster, etc.). ■ Angebot von Begleitung oder Beratung für Jugendliche, die planen, jemanden persönlich zu treffen, den sie online kennengelernt haben. ■ Gemeinsames Erarbeiten von Privatsphäreeinstellungen.

Cybergrooming, Sexting etc. durch Fremde zu sensibilisieren? ■ Wie unterstützen die Fachkräfte in Fällen von Cybermobbing? ■ Wie unterstützen Fachkräfte Kinder und Jugendliche dabei, ihre Privatsphäre zu schützen? ■ Wie werden Kinder und Jugendliche über die Risiken von Blind Dates und Treffen mit nur online bekannten Personen aufgeklärt? ■ Welche Unterstützung bietet die Organisation, um sicherzustellen, dass solche Treffen sicher ablaufen?	

Weiterführende Materialien

- Saferinternet.at: Safer Internet in der Jugendarbeit – wo kann ich mich weiterbilden?
- Saferinternet.at: Fragen und Antworten rund um Peer-Programme
- Studienzentrum Josefstal: Selbstlernkurs zu Digitalen Kompetenzen in der Jugendarbeit
- Youth Policy Labs: Curriculum für digitale Kompetenzen von Jugendarbeit anhand von Digcomp 2.0 (Erasmus Projekt)

7. Datenschutz

Die seit 25. Mai 2018 geltende europaweite Datenschutzgrundverordnung (DSGVO) macht es auch für Einrichtungen bzw. Organisationen der Kinder und Jugendarbeit notwendig, sich vertiefend dem Datenschutz und der Datensicherheit zu widmen. Die folgenden Reflexionsfragen sollen die Kinder- und Jugendarbeit aus dem Blickwinkel des Datenschutzes beleuchten und datenschutzrechtliche Aspekte und Zusammenhänge aufzeigen.

7.1 Datenschutzrechtliche Rollen

Die klare Zuweisung von Verantwortlichkeiten und Zuständigkeiten im Umgang mit Datenschutz gewährleistet eine effektive Umsetzung von Schutzmaßnahmen in der Kinder- und Jugendarbeit.

Mögliche Risiken

- Ein bedeutendes Risiko in der Kinder- und Jugendarbeit entsteht, wenn sich niemand explizit für die Umsetzung von Datenschutzmaßnahmen verantwortlich fühlt. Dies kann dazu führen, dass persönliche Daten von Kindern und Jugendlichen unzureichend geschützt sind, was die Gefahr von Datenschutzverletzungen und Datenmissbrauch durch unbefugte Dritte erhöht.
- Unbefugte Personen könnten Zugang zu sensiblen Daten erhalten, z. B. Zugang von außen (Hacking) oder innerhalb der Organisation (Kinder/Jugendliche verschaffen sich unbefugten Zugriff auf Daten und veröffentlichen diese).

Reflexionsfragen	Mögliche Maßnahmen
■ Wer trägt die Verantwortung für die Umsetzung der Datenschutzregeln gemäß der Datenschutzgrundverordnung (DSGVO)? ■ Wie transparent sind die Zuständigkeiten nach außen? ■ Wer hat Zugriff auf personenbezogene Daten und zu welchem Zweck? ■ Wo werden die Zugriffsrollen definiert und dokumentiert? ■ Sind die Fachkräfte über ihre Zuständigkeiten und Verantwortlichkeiten im Hinblick auf Datenschutz informiert?	■ Zuständigkeiten festlegen. ■ Datenschutzerklärung veröffentlichen – z. B. auf der Website der Organisation oder in Papierformat zum Nachlesen für die Kinder und Jugendlichen. ■ Prüf- und Kontrollverfahren implementieren, um sicherzustellen, dass Datenschutzmaßnahmen effektiv umgesetzt werden (verantwortliche Person). ■ Zutritts- und Zugriffsrollen implementieren. ■ Eindeutige Authentifizierungsverfahren für Fachkräfte einführen, einschließlich der Verwendung von Benutzererkennungen und Passwörtern, um den Zugang zu Datenverarbeitungssystemen zu regulieren. ■ Regelmäßige Schulungen und Sensibilisierungsmaßnahmen von

	Fachkräften im Bereich Datenschutz umsetzen. ■ Verschwiegenheitsvereinbarung einführen, die von allen Fachkräften unterzeichnet wird, um das Bewusstsein für die Bedeutung des Datenschutzes zu schärfen. ■ Bei Ausscheiden von Fachkräften: Rückgabe aller Schlüssel und IT-Geräte sowie Anpassung, Entzug oder Löschung von Zugangsberechtigungen und Zugriffsrechten.

7.2 Speicherung von Daten

In der Arbeit mit Kindern und Jugendlichen wird eine Vielzahl sensibler Daten gesammelt. Diese Daten gilt es effektiv zu schützen, um die Privatsphäre und Sicherheit der Kinder und Jugendlichen zu wahren sowie potenzielle Risiken zu minimieren.

Mögliche Risiken

- Es werden persönliche Daten über Kinder/Jugendliche gespeichert, die für den jeweiligen Anwendungsfall nicht notwendig sind (z. B. um einen Ausflug zu planen, wird das Religionsbekenntnis gespeichert, statt Essenspräferenzen für die Abwicklung der Verpflegung).
- Ein Mangel an regelmäßigen, sicheren Backups kann dazu führen, dass wichtige Daten bei einem technischen Ausfall oder durch Ransomware verloren gehen und somit die Datenwiederherstellung unmöglich ist.
- Die Verwendung von nicht autorisierten Speicherorten wie privaten Laptops, Smartphones oder Cloud-Diensten kann zu unkontrolliertem Zugriff und dem Verlust von sensiblen Informationen führen.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche Daten werden gespeichert? Zu welchem Zweck werden sie gespeichert? Werden Kinder, Jugendliche und Erziehungsberechtige ausreichend darüber informiert? ■ Gibt es klare Verfahren für die Einholung von Einwilligungen bei der Datenerfassung? ■ Gibt es Möglichkeiten, die Speicherung von Daten zu widerrufen?	■ Transparente und verständliche Verfahren bezüglich der Einwilligung, Speicherung (Zweck), Verwaltung (Speicherort) und Löschung von personenbezogenen Daten entwickeln und umsetzen, z. B. im Zuge einer Falldokumentation, Tagesdokumentation, Beratung etc. ■ Prinzip der Datenminimierung einhalten (nur Daten erfassen, die für den

■ Welche Regeln und Prozesse im Umgang mit personenbezogenen Daten sind etabliert und wie werden diese kommuniziert? ■ Wo werden die Daten gespeichert? Auf welchen Geräten? Wo stehen die Geräte? Gibt es abgesicherte Räume? ■ Wie lange werden die Daten gespeichert bzw. wann werden Daten gelöscht? ■ Gibt es Maßnahmen, um die Sicherheit der gespeicherten Daten zu gewährleisten? ■ Wie wird mit Datenschutzverletzungen umgegangen?	festgelegten Zweck unbedingt notwendig sind). ■ Zyklen für das Löschen von Daten festlegen (z. B. Ende eines Projekts, Auszug eines Kindes aus einer WG, Ende einer Prozessbegleitung etc.). ■ Firewalls einsetzen. ■ Regelmäßige Datensicherung (Back-ups) durchführen und sicher abspeichern. ■ Personenbezogene Daten anonymisieren und pseudonymisieren. ■ Notfallmanagement für Datenschutzverletzungen (einschließlich der Meldung an die zuständigen Behörden und der Kommunikation mit den Betroffenen) festlegen und festhalten. ■ Clear Screen Policy: Bildschirme bei Abwesenheit sperren und Bildschirmschoner mit Passwortschutz einsetzen, um unbefugte Einsichtnahmen zu verhindern.

7.3 Weitergabe von Daten an Dritte

Der Austausch personenbezogener oder vielleicht sogar sensibler Daten ist in der Kinder- und Jugendarbeit oft notwendig, um die Zusammenarbeit verschiedener Systeme zu ermöglichen. Ohne klare Richtlinien und Sicherheitsmaßnahmen können jedoch erhebliche Risiken entstehen, die die Sicherheit und das Wohl der Kinder beeinträchtigen könnten.

Mögliche Risiken

- Daten werden unverschlüsselt, z. B. per Mail, weitergegeben und von Unbefugten gelesen oder manipuliert.
- Daten werden an Dritte ohne Zustimmung der betroffenen Person weitergegeben.
- Ohne genaue Dokumentation darüber, wer welche Informationen erhalten hat, kann es schwierig sein, Verstöße oder Datenlecks zu verfolgen oder zu korrigieren.

Reflexionsfragen	Mögliche Maßnahmen
■ Welche Daten werden für welchen Zweck an Dritte weitergegeben?	■ Geeignete Form der Weitergabe festlegen: Nutzung von virtuellen privaten Netzwerken (VPN), E-Mail-Verschlüsselung

■ An wen werden Daten weitergegeben (Erziehungsberechtigte, Schule, Behörden, Systempartner:innen etc.)? ■ Werden die Kinder und Jugendlichen und Erziehungsberechtigen über die Weitergabe der Daten informiert? ■ Wie werden die Daten weitergegeben – über welche Kanäle? ■ Wird der Austausch von Daten dokumentiert, um eine nachhaltige Nachvollziehbarkeit zu gewährleisten?	oder Passwortschutz einzelner Dokumente (PDF-Verschlüsselung, Zip-Verschlüsselung). ■ Transparenz schaffen: Klare Information der betroffenen Personen über die Umstände der Datenweitergabe, einschließlich der Identität der Dritten und des Zwecks der Weitergabe. ■ Austausch von Daten dokumentieren und sicher abspeichern.

Weiterführende Materialien

- Saferinternet.at: Was bedeutet Datenschutz?
- Saferinternet.at: Datenschutz: Tipps und Informationen
- Saferinternet.at: Wie ist der Datenschutz in Europa gesetzlich geregelt?
- bOJA: Leitfaden zur Datenschutzgrundverordnung für Einrichtungen der Offenen Jugendarbeit
- Fachverband Jugendarbeit/Jugendsozialarbeit Brandenburg e. V.: Datenschutz in der Jugendarbeit